PCT / IB 98 / 01855
23. 11. 98

BB98/01855

Europäisches Patentamt | European Patent Office | Office européen des brevets

EJKU

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

98112938.0

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

POTTS

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE

14/10/98

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 98112938.0
Demande n°:

Anmeldetag:
Date of filing: 13/07/98
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
International Business Machines Corporation
Armonk, N.Y. 10504
UNITED STATES OF AMERICA

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Method of transmitting information data from a sender to a receiver via a transcoder, method of transcoding information data, method for receiving transcoded information data, sender, transcoder and receiver

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

METHOD OF TRANSMITTING INFORMATION DATA FROM A SENDER TO A RECEIVER VIA A TRANSCODER, METHOD OF TRANSCODING INFORMATION DATA, METHOD FOR RECEIVING TRANSCODED INFORMATION DATA, SENDER, TRANSCODER AND RECEIVER

The invention relates to a method for transmitting data from a sender to a receiver via a transcoder, which means that the information data is altered and/or reduced before transmitting it to the receiver. The invention further relates to a method for transcoding the information data, particularly for transcoding the information data when it comprises encrypted confidential information data as well as non-confidential information data. The invention also relates to a method of receiving the transcoded information data at a receiver, particularly checking integrity of the information data and trustworthiness of the transcoder. Moreover, the invention relates to a sender, a transcoder and a receiver, combinable to perform transmitting of information data under use of transcoding functionality.

TECHNICAL FIELD AND BACKGROUND OF THE INVENTION

Today, internet-browsing via the world-wide-web is by and large confined to stationary users who have access to browsers running on powerful computing devices such as workstations or PCs. Such devices are not only linked to the Internet via reasonably high-speed and high-bandwidth data connections, but are also equipped with powerful software and hardware for processing and rendering accessible the received multi-media data. Authors make ample use of this infrastructure by creating webpages of ever-increasing complexity, both in terms of the data contents itself which may incorporate a large variety of audio and graphics formats, and executable contents such as applets for advanced functions such as payments, etc.

As users become more accustomed to relying on the web as a general-purpose information source, access to the web is becoming more desirable for users on-the-move, using devices such as mobile telephone handsets or small and lightweight hand-held computing devices. However, users of such devices face problems when trying to access the existing world-wide-web infrastructure: Mobile hand-held devices are connected to the Internet via an unusually slow and fragile data connection. This leads to unacceptably long down-load times for inefficiently formatted data streams.

transcoder cannot be trusted, then the transcoding service is limited to operating on content with little or no value.

Unfortunately, incorporating transcoder functionality into the server or client is unacceptable except for few, highly security-sensitive applications, since it involves upgrades to server software and usually server hardware. In addition, mobile devices evolve at high rates and transcoder functionality is likely to evolve at a similar rate, leading to tight software replacement cycles.

External transcoder services which may be offered as a commercial service by a hand-held-device manufacturer, a data network operator or an ISP, and which could be incorporated with existing proxy-servers, are clearly a more suitable and scaleable solution. Unfortunately, such third-party provided transcoders can rarely be viewed as trusted parties. Security must then be provided by applying end-to-end encryption between the server and the client, leaving the transcoder the impossible task of operating on the encrypted data stream.

In conjunction with existing end-to-end encryption methods, known transcoders cannot be used since they require plain-text access to the entire data stream. Their actions cannot be verified by the clients, thus making them even less applicable for security-sensitive data transfers.

A transcoder is e.g. described in US 5544266. In US 5729293, a device for transcoding coded digital signals which are representative of a sequence of images, which device comprises a variable length decoding channel followed by a variable length encoding and decoding channel, is described. A prediction sub-assembly is connected in cascade between these two channels, and this sub-assembly comprises, in series, between two subtracters a picture memory and a circuit for motion compensation in view of displacement vectors which are representative of the motion of each image. Other implementations are possible, and particularly a scaleable one in which said prediction sub-assembly comprises at least two and more generally a plurality of similar encoding and decoding channels arranged in cascade and corresponding to the same number of image quality levels.

US 5745701 describes a system for interconnecting local networks via a public transmission network, in which equipment items of the microcomputer type, connected to a local network are capable of being connected to the public network by a router in order to communicate

The above explained advantage is increased, when each information data piece is assigned its own piece security information part and piece transcoding-type information part, such that the information data pieces get their own assigned profile, here at least the security- and transcoding-type information. Then the transcoder can individually treat the information data according to its respective profile. Interdependencies between information data pieces is then eliminated.

When an information data piece is assigned its own piece hashing information part, said information data piece being preferably part of said non-confidential information data, again a finer granularity in security can be achieved. Since the hashing implies that the content of the respective information data is not to be altered, only a restricted transcoding functionality can be applied, namely only no transcoding or deletion. Therefore it proves of advantage that such hashing is restricted to the information data where it is in fact needed, such that a maximum transcoding effect can be achieved.

The piece security information parts and piece transcoding-type information parts can be translated into labels according to a translation policy and instead of said piece security information parts and piece transcoding-type information parts, said labels can be transmitted to said transcoder, whereby a policy information, explaining how to interpret said labels, is made available or is already available to the transcoder. The procedure reduces the information to be sent. This is true particularly, where a big number of piece security information parts and piece transcoding-type information parts is to be transmitted, because the saving of data achieved by using the shorter labels is then more and more dominating over the additional data represented by the policy information. This method is comparable to having a short identifier for long to explain actions, like acronyms. The policy information then tells what meaning lies behind the identifier or acronym.

The labels can then be combined in a security- and transcoding-type information packet which is completed by a signature allowing content-integrity-verification at the receiver. This has the advantage that the receiver can make sure if the security- and transcoding-type information packet has been modified or not. If the security- and transcoding-type information packet has not been modified, he can check, whether the received information data has been transcoded according to the rules contained in the security- and transcoding-type

The security- and transcoding-type information packet offers all information which is needed for the transcoder to process the arriving information data correctly. Since the security- and transcoding-type information is not to undergo transcoding, this security- and transcoding-type information packet can be completed with a signature which allows to verify at the receiver if the content of the security- and transcoding-type information packet has been amended somewhere between sender and receiver. Fraudulent or erroneous modification of the security- and transcoding-type information packet can hence easily be recognized at the receiver, which makes the whole information data transmission more secure.

It is an object of the invention according to claim 19 to provide a sender for transmitting data to a receiver via a transcoder which allows using a non-trusted transcoder for transcoding information data which nevertheless can comprise encrypted confidential as well as non-confidential information data.

The sender with the features according to claim 19 has the advantage that although it only needs simple modification with respect to known senders, the advantages of transcoding can be combined with the advantages of secure transmission of security-sensitive, i.e. confidential information data.

A divisor means for subdividing the information data into information data pieces before encrypting and transmitting is relatively easy to implement. Text syntax or image data header information can be used to perform an automatic dividing.

It is an object of the invention according to claim 23 to provide a transcoder for transcoding partly encrypted information data, according to the implied security, hence only accessing content of non-confidential information data.

The transcoder with the features according to claim 23 has the advantage that it is receptive for information data containing encrypted and non-encrypted information data and that it can perform the optimum transcoding possible in that it does not try to access content of the encrypted information data but accesses the non-confidential information data for transcoding. The more the transcoder can dig into the information data, the higher can be the transcoding efficiency due to a preciser knowledge in the transcoder, which information can be reduced to which extent. However, encrypted information data is not accessible to such content analysis which is as intended by the sender. The necessary information how to treat which

In addition, the system is flexible in that the policy regarding the transcodability and security of individual data fields can be specified by the server.

Furthermore, the actions performed by the transcoder can be verified to the extent that the transcoder has only content modified according to a stated policy. The assumption made here is that the secure fields of the content require no transcoding.

The solution is applicable to scenarios where electronic commerce, on-line banking, or other security-sensitive applications are run on Tier-0 or Tier-1 clients with limited input or output capabilities and bandwidth-limited connections to the servers, without requiring the servers to install and maintain a dedicated and trusted transcoder function, or where rapid development cycles for new and improved device capabilities and therefore transcoder functions are expected and where independent transcoder-services are therefore preferred.

Starting from an original information data stream which is divided into data fields, also called information data pieces, the herein proposed method can comprise the following steps:

- Inserting additional tags, respectively labels, into the original data stream that mark the data fields in terms of their transcodability, e.g. transcodable, non-transcodable, optional, critical, etc., and their security relevance, e.g. security-sensitive, not security-sensitive, etc., these labels being herein referred to as security labels or piece security information part label and piece transcoding-type information part labels.

- Generating a policy document which defines the transcoder-allowed operations for each tag. This policy document or policy information hence provides for the explanation of what the labels mean, how they should be interpreted. This step can be left out if the policy is inherently known in the transcoder.

- Separating the security-sensitive information fields and applying end-to-end encryption on those selectively and individually, leaving the non-security-sensitive information fields unencrypted.

- Generating a document summary, also referred to as security- and transcoding-type information packet, based on the structure of the original input stream, hence including the security labels and transcoding-type labels.

After the field decomposition is complete, the server 1 then attaches or assigns two classes of labels to each field f_i. The first label class L_s is a security label, also called piece security information part, which indicates whether the given field f_i is to be encrypted at the time of transmission. For example, the set of possible security labels L_s could be defined as

$$L_s = \{ \text{secure, non-secure} \} \quad (1)$$

and $L_s(f_i) \in L_s$ where $L_s(f_i)$ is the security label of f_i. The label L_s could be extended in several ways such as to include, for example, levels of encryption, e.g. with short or long keys, to include authentication information or to include a signature.

The second label class L_t is a transcoding label, also called piece transcoding-type information part, which indicates what action the transcoder 2 may take when a content field is received. For example a possible set of transcoding labels L_t could be defined as

$$L_t = \{ \text{non-transcodable, transcodable, critical, non-critical} \} \quad (2)$$

where the exact meaning of these labels would be defined in a translation policy associated with the server 1. For example one such policy may be to interpret the transcoding labels L_t as follows:

`transcodable' implies that the content field can be transcoded at the transcoder's discretion:

`non-transcodable' implies that the transcoder 2 is not to alter the content field received from the server 1;

`critical' implies that the field must be sent to the requesting client 3 from the transcoder 2;

`non-critical' implies that the transcoder 2 may delete the content field from the content forwarded to the requesting client 3.

The server 1 may issue a policy statement pol(S) which contains the set of security and transcoding labels, $L_s(S)$ and $L_t(S)$ respectively, and also a clear statement as to how the labels are to be interpreted. Since the policy statement pol(S) contains no security-sensitive information, it can be retrieved at any time from the server 1, and cached for later use in a connection to the server 1 for content retrieval.

Here it is assumed that the translation policy has been chosen such that it follows the rules of the policy information 17 already known and accessible for the transcoder 2. Therefore no

later assignment of the labels to the corresponding information data pieces, namely in the transcoder 2 and the receiver 3. The labeling means or labeler can be fed with user preferences to give the labeler an input about which information data pieces shall be encrypted and/or transcoded and how. So labeling can depend on some automatic system which automatically assigns the respective labels, e.g. following some implemented rules and/or depend on given rules or individual labeling preferences, given by a user or derived from a list. Sometimes labeling can be done by following a fixed labeling scheme and sometimes a individualized labeling list might be the optimum solution to tell the labeler which label value it has to stick to which information data piece.

Herein the group of all security labels is referred to as group of piece security information parts, denoted with SIL, while the group of transcoding labels is referred to as group of piece transcoding-type information parts, denoted with TIL. With other words, each field, respectively information data piece, has its piece security information part, whereby all piece security information parts together form the security information. The security information can be split up into the group of all security labels and the corresponding translation policy information. Hence, for each field the piece security information part can be also split up into the security label and the corresponding translation policy information, short policy information.

The TIL together with the corresponding policy information forms the transcoding-type information 13, which in the figure is depicted in a simplified form. The SIL together with the corresponding policy information forms the security information 12, which in the figure is also depicted in a simplified form. The principle is that the transcoder 2 shall be provided with all information needed for performing the transcoding according to the sender's wish which is expressed in a form that the transcoder 2 can understand and interpret for correct execution. This means that the security information 12 and the transcoding-type information 13 are transmitted to the transcoder 2 either in the label form which implies that the transcoder 2 understands the labels, either because the transcoder 2 already has the corresponding translation policy available, or is designed to understand the labels directly or is or has been provided with the policy information 17 by the sender 1 or by any other institution, or that in the case, a policy-label split version is not desired or realizable for whatever reason, the non-labeled security information 12 and the non-labeled transcoding-type

Without loss of generality it is assumed that the first j fields f_1, f_2, ..., f_j are labeled as secure, while the remaining fields f_{j+1}, f_{j+2}, ..., f_N are labeled as non-secure. The server 1 then forwards the following tuple to the transcoder 2:

$$< \text{sum}(D), \text{sign}(\text{sum}(D)), E_K(d(f_1)), ..., E_K(d(f_j)), d(f_{j+1}), ..., d(f_N) > \quad (7)$$

where $d(f_i)$ is the data associated with field f_i, and $E_K(d(f_i))$ is the encryption of the data associated with field f_i under the encryption key K. The data of each secure field is encrypted individually.

The transcoder 2 comprises decision means 4, denoted with TC, for deciding which part of the received partly encrypted information data 14, 15 is to be transcoded before transmitting it to the receiver 3.

Hereby the encrypted confidential information data 14 is only transcodable without using its content while the non-confidential information data 15 is transcodable, having access to its content.

In principle, transcoding means that the received encrypted confidential information data 14 is reduced in its size or complexity. This can be done in various levels, such as a very strong transcoding, resulting in an absolutely minimized version of the encrypted confidential information data 14 and the non-confidential information data 15 , and to the opposite a rather lean transcoding, reducing the encrypted confidential information data 14 and the non-confidential information data 15 only to some minor extent. Transcoding can comprise data compression or partial data deletion. Here, the security- and transcoding type information 12, 13 is read from the security- and transcoding type information packet 11 and used for transcoding the encrypted confidential information data 14 and the non-confidential information data 15 leading to transcoded encrypted confidential information data 24, denoted with TECD, and transcoded non-confidential information data 25, denoted with TNCD.

The transcoder 2 here operates on the received data stream 14, 15 in two passes. In the first pass, the transcoder serializes the data by removing subfield structure from each field. For example, if f_i is a field and $f_{i,j}$ a subfield of f_i, this serializing can be thought of as performing the following operation

$$d(f_i) = < . , d(f_{i,j}), . > \text{----->} < . < \text{ptr} >, . >, \text{ptr: } <d(f_{i,j})>. \quad (8)$$

The structure of the original content D as it existed on the server 1 is represented in sum(D), which the client 3 can verify by checking the server's signature sign(sum(D)) on sum(D). Thus the client 3 is able to determine the set of fields that represent D, as specified by the server 1. Further, since the security- and transcoding type information packet sum(D) contains the label tuples for each field of the content D, the client 3 may verify the labeling that the server 1 chose for the fields of the content D. In particular, the client 3 can determine which fields were designated as secure by the server 1, and which were designated as transcodable by the server 1.

The client 3 then checks that all fields that were specified in the security- and transcoding type information packet sum(D) as secure and critical, have not been deleted or modified by the transcoder 2 in the transcoded encrypted information data $T(E_K(d(f_1)), ..., E_K(d(f_j)))$. Here, at least part of this verification is provided by the encryption algorithm E which may include authentication information about the data that was encrypted.

Also, the client 3 can compare the set of transcodable fields as specified in sum(D) with the received fields $T(d(f_{j+1}), ..., d(f_N))$ to verify that the transcoding process has not deleted or inappropriately modified any content that could be represented at the client 3.

6. Method according to claim 4 or claims 4 and 5, characterized in that the piece security information parts and piece transcoding-type information parts are translated into labels (SIL, TIL) according to a translation policy, that instead of said piece security information parts and piece transcoding-type information parts, said labels (SIL, TIL) are transmitted to said transcoder (2), whereby a policy information (17), explaining how to interpret said labels (SIL, TIL), is made available or is already available to the transcoder (2).

7. Method according to claim 6, characterized in that the labels (SIL, TIL) are combined in a security- and transcoding-type information packet (11) which is completed by a signature (10) allowing content-integrity-verification at the receiver (3).

8. Method of transcoding in a transcoder (2) partly encrypted information data (14, 15) received from a sender (1) and to be transmitted to a receiver (3), whereby said partly encrypted information data (14, 15) comprises non-confidential information data (15) and encrypted confidential information data (14), and is accompanied by security information (12) and transcoding-type information (13), which is used for deciding which part of said partly encrypted information data (14, 15) is to be transcoded before transmitting it to said receiver (3), whereby said encrypted confidential information data (14) may only be transcoded without using its content while said non-confidential information data (15) may be transcoded, having access to its content.

9. Method according to claim 8, characterized in that the partly encrypted information data (14, 15) is received subdivided into information data pieces.

10. Method according to claim 9, characterized in that each information data piece has assigned its own piece security information part and piece transcoding-type information part.

11. Method according to claim 10, characterized in that the piece security information parts and piece transcoding-type information parts arrive in the form of labels (SIL, TIL) and that for transcoding, a policy information (17) which is available to the transcoder (2) is used, which explains how to interpret said labels (SIL, TIL).

18. Method according to claim 17, characterized in that a content-integrity-verification of a security and transcoding-type information packet (11) comprising the labels (SIL, TIL) is performed using a signature (10) thereof.

19. Sender (1) for transmitting information data (9) to a receiver (3) via a transcoder (2), which transcodes said information data (9) before transmitting it to said receiver (3), said information data (9) comprising confidential information data (16) and non-confidential information data (15), characterized in that said sender (1) comprises an encryptor (5) for encrypting said confidential information data (16), and that together with the partly encrypted information data (14, 15) to said transcoder (2), security information (12) and transcoding-type information (13) is sendable, being usable by said transcoder (2) for said transcoding, whereby said encrypted confidential information data (14) is transcodable without using its content while said non-confidential information data (15) is transcodable, having access to its content.

20. Sender (1) according to claim 19, characterized in that it comprises divisor means (21) for subdividing the information data (9) into information data pieces before encrypting and transmitting.

21. Sender (1) according to claim 20, characterized in that each information data piece has assigned its own piece security information part and piece transcoding-type information part and that instead of said piece security information parts and said piece transcoding-type information parts, to said transcoder (2), labels (SIL, TIL) are transmittable, into which according to a translation policy, said piece security information parts and said piece transcoding-type information parts are translatable, whereby a policy information (17), explaining how to interpret said labels (SIL, TIL), is deliverable or is already available to the transcoder (2).

22. Sender (1) according to claim 21, characterized in that it comprises a packetizer (23) for combining the labels (SIL, TIL) in a security- and transcoding-type information packet (11) and a signature-generator (22) for completing said packet (11) by a signature (10), which allows content-integrity-verification at the receiver (3).

26. Receiver (3) according to claim 25, characterized in that the transcoded partly encrypted information data (24, 25) is received subdivided into information data pieces, that the piece security information parts and piece transcoding-type information parts arrive in the form of labels (SIL, TIL) and that with the comparison means (7), under use of a policy information (17) which is available to said receiver (3) and a policy information interpreter (8), said labels (SIL, TIL) are interpretable and that thereby the correctness of the transcoding is testable.

27. Receiver (3) according to claim 26, characterized in that a content-integrity-verification of a security and transcoding-type information packet (11) comprising the labels (SIL, TIL) is performable with an integrity-check means (6) using a signature (10) of said packet (11).

1/1

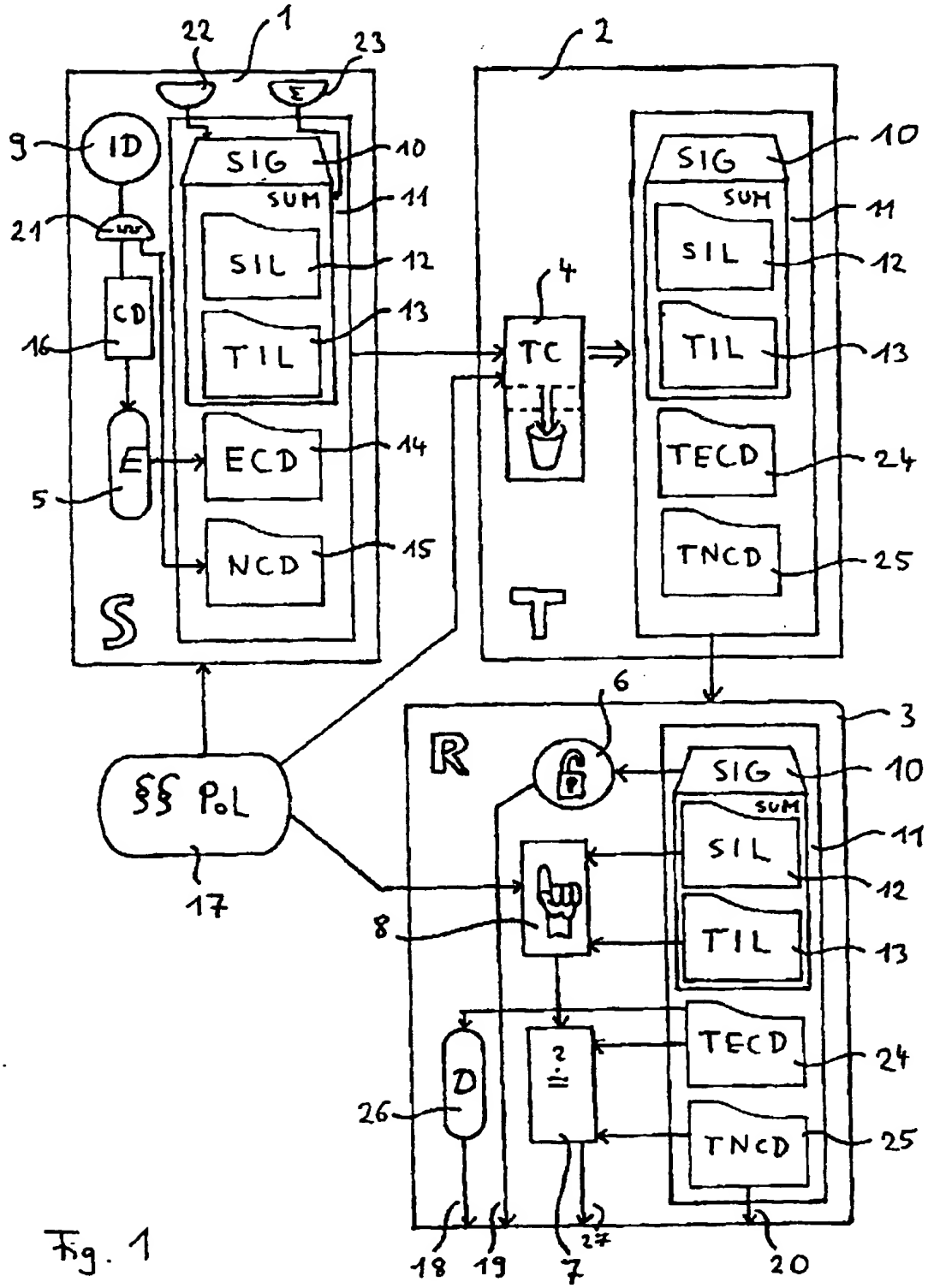
22
1
23
2
9
ID
SIG
10
SUM
11
21
SIL
12
CD
16
TIL
13
4
TC
E
ECD
14
5
TECD
24
NCD
15
TNCD
25
S
T
6
3
R
§§ PoL
17
8
D
26
?
=
18
19
7
27
20

Fig. 1